Keynote Speech of David W. Mills, Assistant Secretary for Export Enforcement

UPDATE Conference, July 30, 2014

Good afternoon. It is a pleasure for me to speak at the 2014 BIS annual Update Conference. The Administration has accomplished a significant amount of regulatory reform over the year, the highlights of which are the transfer of certain military aircraft, vehicles, and ships and related parts and components to the Commerce Control List, and the impending transfers of satellite-related and certain military electronics items before the end of 2014. I recognize that these transfers result in short-term complexities for companies, particularly with regard to the reclassification of items, but the long-term benefit for diligent and law-abiding exporters will be significant.

In addition to the challenges to industry, the transfer of items from the ITAR to the EAR presents new enforcement challenges for the U.S. Government because of the more flexible licensing authorizations that may be available. We are addressing these challenges, in part, through what former Secretary Gates referred to as "higher walls" to secure trade that promotes interoperability with our allies, discourages the design-out of U.S.-origin items, and allows the U.S. Government to focus its resources on the most sensitive transactions. That's where my organization comes into play.

The Role of Export Enforcement

For those new to the EAR, and even for our more experienced exporters, I think it is important to frame the context of Export Enforcement's role at the Bureau of Industry and Security. We work to ensure that strategic trade is secured by an effective export control system based largely on multilateral control lists that deters, prevents, and redresses the diversion of dual-use and munitions items to end users and for end uses involved in the development of weapons of mass destruction and advanced conventional weapons or that support international terrorism. We want to promote secure trade that is in the national interest of the United States. To that end, our law enforcement program focuses on sensitive exports to hostile entities or those that engage in onward or inward proliferation.

Over these past 32 years, Export Enforcement at BIS has evolved into a sophisticated law enforcement agency, with criminal investigators and enforcement analysts working together with licensing officers to identify violations and redress them. Using our subject matter expertise in the area of export controls, coupled with our unique and complementary administrative enforcement tools, as well as our partners in other agencies, industry, and abroad, we have leveraged our authorities to maximize the impact we are having.

BIS maintains Special Agents at offices in 14 cities across the United States, including four locations where we have agents co-located with the Federal Bureau of Investigation. Most recently, we are assigning an agent to work out of the offices of

the Defense Criminal Investigative Service (or DCIS) in San Antonio, and we're very proud to be working hand in hand with the Department of Defense.

BIS also has seven Special Agents assigned with the Department of Commerce's Foreign Commercial Service to conduct end-use checks to safeguard the disposition of U.S.-origin items exported abroad. These Export Control Officers or ECOs are assigned to six strategic locations that are critical to our mission: China, the United Arab Emirates (UAE), India, Russia, Singapore, and Hong Kong. All of these ECO positions have regional responsibilities that extend their reach to an additional forty-three countries and I am pleased that all seven are presenting here at Update. Please take advantage of their

country and regional expertise to facilitate your exports to and through these destinations.

The talented personnel that BIS has cultivated is only one of our strengths. As I spoke of previously, our administrative enforcement tools are also unique. The EAR places legal responsibility on persons who have information, authority or functions relevant to carrying out transactions subject to the EAR. These persons may include exporters, freight forwarders, carriers, consignees, and other participants in an export transaction. The EAR applies not only to parties in the United States, but also to persons in foreign countries who are involved in transactions subject to the EAR. And with the President's Export Control Reform initiative in full swing, our responsibilities are significantly increasing with the transfer of tens of thousands of military parts and components from the

ITAR to the EAR, many of which can be exported without a license subject to certain safeguards.

Higher Wall Initiatives

Two key interagency efforts contribute to the higher fence paradigm: the Information Triage Unit housed in our Office of Enforcement Analysis and the Export Enforcement Coordination Center, or E2C2, housed at the Department of Homeland Security.

Since it went into operation in mid-2012, the ITU has evaluated foreign parties to license applications, producing more than 2,100 reports on their bona fides. It is safe to say that when the ITU gets involved with licenses for the most sensitive

transactions, the U.S. Government's ability to evaluate the bona fides of the foreign parties is significantly improved, thereby facilitating the processing of these license applications as well as securing the integrity of our export control system.

Moreover, the ITU has provided important analysis to support Entity List nominations and to review appeals resulting from such designations. Entity List designations prohibit U.S. exports to listed parties absent U.S. Government authorization. Recent ongoing ITU activities include working with the End-User Review Committee to identify Ukrainian and Russian parties undermining stability in Ukraine, UAE parties supporting foreign terrorist organizations, and Haqqani network actors implicated in improvised explosive device incidents involving U.S. and coalition troops.

The E2C2 has been similarly effective in bringing better coordination of export enforcement investigations. Deconfliction involves law enforcement agencies exchanging information about new cases to determine if any other U.S. Government agency already has an investigation related to the same matter or possesses information that will aid in the investigation. Since its existence, the E2C2 has deconflicted over 3,100 cases, thus helping us work more effectively and efficiently with our FBI and Homeland Security colleagues.

In addition, Export Enforcement has significantly increased the consequences to companies we are not able to verify during our end-use checks by strengthening the Unverified List or UVL,

further enhancing our higher walls initiative. In December 2013, we amended the UVL to make it a more useful tool for exporters to identify foreign parties whose bona fides cannot be confirmed by the U.S. Government and instruct them how to deal with those parties. For transactions normally subject to a license exception, where a UVL party is involved, the exporter must seek a license from BIS. For all other transactions not subject to a license requirement, the exporter must obtain a statement from the UVL party certifying compliance with the EAR and agreeing to host an end-use check. That will assist BIS in determining the bona fides of the party. On June 16, 2014, we published the first set of UVL designations from China, Hong Kong, Russia, and the United Arab Emirates.

We are also continuing to work closely with our colleagues at the Directorate of Defense Trade Controls to coordinate end-use checks where EAR items, such as those under the 600 Series, are co-located with ITAR items. This will avoid duplication of resources and allow the U.S. Government to obtain a more fulsome picture of the activities of foreign parties involved with U.S. exports.

Vital Role of Industry

In the context of these initiatives, industry REMAINS the first line of defense. Industry reports of suspicious transactions have led to the identification and disruption of some of the most sophisticated and dangerous proliferation networks. Our special agents will tell you that some of our best cases start

from industry sources. Without the cooperation of industry, these bad-actors might have continued to operate unabated. I strongly encourage you to report suspicious transactions through our website or by contacting the closest Office of Export Enforcement (OEE) field office.

Last year, I discussed with you our plans to expand outreach to companies involved with the transfer of munitions items to the CCL. Since the last time I spoke to you here, OEE has conducted approximately 1,500 outreaches and tailored our outreach materials to include the new 600 Series requirements. Your knowledge and compliance with the EAR establishes a built-in warning system for Export Enforcement to be aware of suspicious actors.

Coupled with this general outreach, Export Enforcement has expanded its Guardian outreach program to industry over the past two years, where we alert companies of suspicious parties that may be seeking to obtain your items. We fully appreciate the reputational risk associated with your items being involved in illicit activities, and this advance warning system is meant to help you identify otherwise unforeseen risks in potential transactions.

Cybersecurity Initiative

In February, I announced a new area of focus -- cyber-intrusions and data exfiltration that result in your export controlled data ending up overseas. As President Obama recently stated, "the

Cyber threat is one of the most serious economic and national security challenges we face as a nation. America's economic prosperity in the 21st century will depend on cyber security."

The perpetrators of cyber-crime are varied; they include independent hackers, criminal organizations as well as state actors. Let me be clear, the theft of export-controlled information from your computer systems as a result of foreign cyber actors is a threat to U.S. national security interests and your company's competitive lifeblood: intellectual property.

Yesterday, Export Enforcement hosted an interagency panel on "Cyber Threats to Industry." Interagency officials discussed cyber security best practices, including the new NIST Cyber Security Framework, mechanisms for reporting cyber crimes via

the FBI's iGuardian reporting portal, and DHS mitigation and response resources.

A key aspect in this regard is understanding that reporting to Export Enforcement the exfiltration of controlled technology is separate and distinct from submitting a voluntary self-disclosure (VSD). The latter involves your discovery of a violation of the EAR committed by your company. By reporting cyber thefts, you are giving us critical information that can allow BIS, working with our interagency partners, to identify these cyber-actors and bring our unique BIS tools to bear against them. I believe that cyber security, like effective export controls can only be achieved effectively with your support and partnership.

Returning to VSDs, let me continue to reinforce that the best way to ensure you're not violating the regulations is to have a comprehensive internal compliance program (ICP) in place. A good compliance program pays for itself: it keeps you from committing a violation in the first place; and if you do slip up, it will be a mitigating factor in our analysis of the case.

An ICP ensures that all employees involved with exports understand the EAR and know that senior management is committed to compliance with the regulatory regime. Other key aspects of the ICP are knowing your customers, asking them for end-use certificates, and effectively screening them against government lists.

Let me highlight specific actions you should be taking in this regard:

1) All transactions should be screened against government lists. A consolidated list is available for free at www.export.gov/ECR.
2) All items subject to an export transaction should be classified against the Commerce Control List (or CCL) and sales persons need to understand list-based, end use, and end user controls.
3) For items subject to a license, you have an obligation to share license conditions with your customer and I highly encourage you to ensure they acknowledge their intent to comply, even where such acknowledgement is not otherwise required by BIS. Our end-use checks over the

past year have found significant non-compliance in this area.

4) For license exception transactions involving Strategic Trade Authorization (STA), ensure that you obtain the certification from your consignee before you ship in which the recipient acknowledges that it understands that any subsequent retransfer or reexport requires a similar consignee statement prior to such retransfer or reexport.
5) For export transactions with end use or end user concerns, we recommend that you obtain end use certificates and double check potential licensing requirements. Self-blinding by not inquiring about end use or not doing due diligence on an end user is not an acceptable defense.
6) Finally, for items moving through transshipment locations like Hong Kong, Singapore, and the UAE, it is important for

you to understand the foreign export control requirements of those governments in addition to those of the EAR. BIS has published a new best practice encouraging exporters to obtain a copy of their Hong Kong and UAE customers' import licenses prior to exporting and to ensure that your customers in these three transshipment locations are aware of export control requirements for the reexport, transshipment, or transit of your item.

For Hong Kong, the absence of receipt of such an import certificate for any multilaterally-controlled item from the importer should be a red flag, as it should be with regard to certain controlled items in the UAE, like CWC chemicals and nuclear-related items. In Hong Kong, we have encountered many entities that are nothing more than

secretarial firms who simply offer a forwarding service for the reexport of your item to another country. Because of the likely difference in licensing treatment for your item to Hong Kong as compared to most other countries, such as China, extra due diligence is warranted.

General Compliance Trends

I recognize there has been some angst in the export community about the compliance philosophies of BIS versus DTC with regard to military items. Let me first say that overall, since USML items started transitioning to the CCL in October 2013, I have been impressed with the diligence of exporters to comply with the 600 series controls.

As of today, only 18 VSDs have been filed with BIS under the 600 Series. Without pre-judging the matter, however, it is my sense that we will handle the 600 Series VSDs in a manner very similar to that of DDTC and that most will result in a warning letter or no action at all, as is the case with most VSDs previously filed under the EAR.

What this issue primarily speaks to is how the two agencies handle cases under the doctrine of strict liability, which I believe to be substantially the same. But there is also a realm of cases that fall between this category - where no aggravating factors are present - and a criminal prosecution. As we become more familiar with the nature of VSDs filed under the 600 series, it is my intention, as previously stated, to issue new BIS Administrative Enforcement Guidelines modeled upon those

promulgated by the Office of Foreign Assets Control (OFAC). OFAC has a robust and comprehensive administrative enforcement program for cases involving more serious violations. Their Guidelines - premised upon the statutory criteria set forth in IEEPA, the statutory authority pursuant to which both agencies now administer and enforce their respective regulations - uses the transaction value to determine the baseline for assessing a civil penalty. The OFAC Guidelines also provide greater transparency and predictability for the exporting community, an important objective of ECR.

So you may expect to see a continuing robust and comprehensive administrative enforcement program at BIS involving cases where aggravating factors are present, apart from cases involving knowledge and willful conduct, whether or

not those cases arise in the context of criminal prosecutions. Such factors include inadequate compliance programs, systemic failures in those programs, harm to U.S. national security or foreign policy interests, and, I might add, improperly pronouncing our acronyms, particularly "BIS" and "EAR.""

Export Enforcement is committed to assisting legitimate exporters comply with the EAR while focusing its resources on the most egregious violations – those cases where companies and individuals are purposely skirting the rules or the exports caused harm . As Under Secretary Hirschhorn says, “Those who comply with the rules benefit from strong enforcement because lax enforcement permits violators to flourish.” Let me now turn to actions we are taking to stop these violators.

ENFORCEMENT CASES

Since our conference here last year, we have had some very significant cases recently concluded across a spectrum of issues and destinations.

Weatherford International Ltd.

Our biggest civil penalty in the past year, in fact the biggest ever, was levied against Weatherford International Ltd. in Houston, Texas, and four of its subsidiaries who agreed to pay a combined $100 million for export control violations involving Iran, Syria, Cuba, and other countries. A $50 million civil penalty was imposed for the export of oil and gas equipment to Iran, Syria, and Cuba in violation of the EAR and the Iranian

Transactions and Sanctions Regulations (ITSR). BIS also alleged that Weatherford exported items controlled for nuclear non-nonproliferation reasons to Venezuela and Mexico. The Department of Justice imposed a $48 million monetary penalty on Weatherford International Ltd. pursuant to a deferred prosecution agreement entered into on November 26, 2013, and also imposed $2 million in criminal fines pursuant to guilty pleas by two of Weatherford's subsidiaries. Weatherford agreed, as part of the settlement, to hire an unaffiliated third-party expert in U.S. export control laws to audit its compliance with respect to all exports or re-exports to Cuba, Iran, North Korea, Sudan, and Syria for calendar years 2012, 2013, and 2014. The Weatherford investigation was conducted by OEE at BIS, working closely with OFAC and the Department of Justice.

Ming Suan Zhang

On December 10, 2013, as a result of a joint investigation by OEE and HSI at the Department of Homeland Security, Ming Suan Zhang, a citizen of the People's Republic of China, was sentenced to 57 months incarceration and a forfeiture of $1,000 for violating the International Emergency Economic Powers Act by attempting to export high-grade carbon fiber from the United States to China. This material can be used in the production of such items as ballistic missiles, unmanned aerial vehicles, and nuclear centrifuges. In this particular case, Zhang attempted to negotiate a long-term contract for massive quantities of the controlled commodity, which he asserted was to be provided to a Chinese company involved in the development of a military fighter aircraft.

Amplifier Resarch

Last year I told you about Timoth Gormley, the export control officer at Amplifier Research who was sentenced to 42 months in prison, admitting that he had: altered invoices and shipping documents to conceal the correct classification of amplifiers to be exported so that they would be shipped without the required licenses; listed false license numbers on export paperwork for defense article shipments; and lied to fellow employees about the status and existence of export licenses. On September 26, 2013, BIS denied Mr. Gormley's export privileges for 10 years based on his conviction.

On January 17, 2014, BIS reached a settlement with Amplifier Research for a $500,000 penalty. However, BIS suspended the

civil penalty in its entirety because of the VSD filed by Amplifier Research in 2011 detailing the actions of Gormley and its substantial cooperation in the course of this investigation. The settlement also mandates that Amplifier Research hire an expert outside of the company to conduct an audit of its compliance with export control laws, including recordkeeping. By filing the VSD, Amplifier Research avoided criminal charges (against the company itself), and the suspended fine will be waived at the end of the penalty period provided all commitments are met.

Karl Lee

Finally, on April 29, 2014, The Justice Department unsealed an indictment of Chinese proliferator Li Fangwei, a.k.a. Karl Lee

and the State Department announced a $5 million bounty for his arrest. The indictment identified Lee as a "principal contributor" to the Iranian ballistic missile program. In a coordinated U.S. Government action, BIS announced on the same day that we were adding eight Chinese companies and one Chinese individual to its Entity List for their roles in supplying Iran's ballistic missile program and OFAC added eight of Karl Lee's front companies to its List of Specially Designated Nationals and Blocked Persons.

These are just a few of the cases OEE agents investigated in the last year. In fiscal year 2013, BIS investigations led to the criminal convictions of 52 individuals and businesses for export violations with penalties of over $2.6 million in criminal fines, more than $18 million in forfeitures, and more than 881

months of imprisonment. In addition, we completed 63 administrative export cases, resulting in $6.1 million in civil penalties. Export Enforcement also supported the addition of 68 new parties onto the BIS Entity List.

Outlining these cases once a year at Update is important, but even more effective is companies having access to a compilation of our enforcement actions for reference and training purposes. I am pleased to report that we have just updated and republished *Don't Let This Happen To You*, which sets forth information regarding our organization, its role and authorities, and a number of cases highlighting our enforcement activities pursuant to the EAR. This revised document is now available on the BIS website. These case

successes demonstrate the judicious vigor with which we use our criminal and civil authorities to secure U.S. trade and enforce the Antiboycott regulations.

Office of Antiboycott Compliance

Finally, no picture of Export Enforcement is complete without reference to the Office of Antiboycott Compliance (OAC). OAC carries out its mandate through a threefold approach: counseling U.S. businesses on the substance and application of the EAR to particular transactions; monitoring the type and origin of boycott requests received by US businesses; and bringing enforcement actions and imposing penalties, where necessary. In addition to these traditional activities, OAC partners with the Office of the U.S. Trade Representative and the U.S. Department of State and U.S. Embassy officials to engage directly with Ministries, Chambers of Commerce and businesses in boycotting countries in an effort to discourage inclusion of boycott-related terms and conditions in

commercial documentation at the source, to prevent violations before they occur.

OAC may impose civil penalties against U.S. businesses for taking actions in furtherance or support of an unsanctioned foreign boycott or for failing to report the receipt of a boycott-related request. In its case against Baker Eastern, SA (Libya), for example, OAC alleged that, Baker Eastern, on twenty-two occasions, furnished to Libyan customs in Libya a Certificate of Origin, each of which contained a statement regarding compliance with the Arab Boycott of Israel, as well as two items of prohibited information: a negative certificate of origin regarding the goods, and a blacklist certification regarding the producing company. Because Baker Eastern voluntarily

disclosed these transactions to OAC and maintains an exceptional multinational compliance program, the company benefited from great weight mitigation in accordance with the Antiboycott Penalty Guidelines.

Similarly, in its case against Digi-Key Corporation, OAC alleged that the company furnished prohibited information in a negative certificate of origin which contained a statement that certain of the ordered goods were not made in Israel and, on fifty-eight occasions, failed to report receipt of a directive prohibiting any import from, or goods made in, Israel. Digi-Key likewise voluntarily disclosed these transactions to BIS and benefited from great weight mitigation in accordance with the antiboycott Penalty Guidelines.

These cases are representative of the kinds of antiboycott issues any company might confront in doing business in a boycotting country and, even more importantly, of the benefit of voluntarily disclosing fully and promptly should a company discover a violation.

OAC continues to analyze trends with respect to the origin and type of boycott-related requests received by U.S. persons in letters of credit, purchase orders, and other commercial documents. Since our last UPDATE, OAC reports that the United Arab Emirates remains the leading source, but that Iraq has moved into second place with a dramatic spike in prohibited boycott requests appearing mostly in Invitations to

Bid and patent registrations. Bangladesh and Qatar also figure prominently as sources of boycott-related requests.

Of course, if anyone has any boycott issues or concerns in a transaction, OAC is available through their Advice Line to counsel and guide you.

CONCLUSION

Successfully erecting higher fences under the President's Export Control Reform initiative is dependent upon BIS collaborative efforts with industry, our interagency colleagues, and international partners. We are committed to its success, which ultimately safeguards U.S. national security and economic security. I recognize this is a challenge, especially in the short

term, with regard to the substantial number of changes. But attending workshops, implementing a robust ICP, and reporting unauthorized activities is the best way to protect your company's reputation and allow Export Enforcement to protect our national security interests. It can be said that we at BIS "play defense on the Commerce Department's export promotion team." Your help in securing America's exports is a win-win proposition. Thank you very much for your attention today, and I wish you success with your lawful exports!